

PATENT APPLICATION

System for Controlling the Use of Licensed Software

Inventor: Steven Karl Schoch
974 Bluebonnet Drive
Sunnyvale, California 94086
Citizenship: United States

Inventor: Paul Swart
3470 Canyon Creek Drive
San Jose, California 95132
Citizenship: Netherlands

Assignee: Starnet Communications Corporation
1270 Oakmead Parkway, Suite 301
Sunnyvale, California 94086
Incorporation: State of California

Entity: Small

5 **System for Controlling the Use of Licensed Software**

BACKGROUND OF THE INVENTION

 This invention relates to a system for controlling the use of software
licensed to a user for use on a user's system. In particular it relates to a system which
10 permits the software publisher to control copying of the software it licenses to preclude
users from giving away "free" copies to others.

 With advances in computing power and increasing research and
development costs, sophisticated software is now widely available even for use on
personal computers. Such software is highly portable, being easily disseminated over the
15 Internet, or distributed by CD-ROM or other means. This, unfortunately has resulted in
widespread unauthorized copying of licensed software. Because of the considerable costs
of research, development, marketing, etc., the software publisher desires to prevent such
unauthorized copying, and to control the use of the software in accordance with the terms
of the license.

20 The publisher of software typically licenses a user to use the software on
a single system, and to make a back-up copy. The user, on the other hand, sometimes
chooses to ignore the license terms and use the licensed software on many systems, or
provide free copies to friends etc. This is a major problem with many game programs,
and is a significant problem with many types of conventional business software. In view
25 of the huge size of the software market, it is not surprising that many solutions have been
proposed for controlling the use of such software to prevent unauthorized copying.

 One approach, often used with expensive programs, is to provide a
hardware device, commonly called a dongle, which the user attaches to the computer
upon which the software is to operate. Each time the software runs on that computer, it
30 checks to see if the hardware device is present. If the hardware device is not present, then
the software does not operate. The hardware device typically includes something, for
example, an integrated circuit, which is difficult or expensive for users to counterfeit.
Unfortunately, an undesirable side-effect of this approach is that the cost of the dongle
adds an additional \$10 to \$25 per license for use of the software. It also adds overhead to

the management of the licenses, because user's devices occasionally malfunction requiring replacement with a new appropriate code numbered dongle. Furthermore, many software companies do not have engineering capabilities for manufacturing such dongles in-house. Such solutions also cause fears of inconvenience in the consumer.

5 Other systems provide key numbers which may be unique to a user, but are not restricted to the user's system. Before the software can operate the user must enter the appropriate key, for example, a number on a floppy disk or CD-ROM provided with the software. Such systems are easily circumvented by passing along the key number with the copy of the software.

10 Still other techniques employ encryption technology to make duplication of the software more difficult, and preclude copying with ordinary operating system copy techniques. Without the proper encryption software, the user is unable to make a functional copy of the software provided by the publisher.

15 Another approach used on some network software is to control the number of users on a system. In such systems, a business is licensed to have a previously agreed upon number of copies of a particular piece of software operating from a server at any given time. As each user logs in or out of using the program, their presence is counted, and appropriate controls are applied through the server to assure that the number of users at any given time does not exceed the license limit.

20 The end result of the approaches discussed above is that no low-cost system really provides satisfactory protection to the software publisher, or the needed flexibility to the user.

SUMMARY OF THE INVENTION

25 This invention provides a unique system and method for controlling the distribution of software under a license agreement. By identifying the computer utilized by the licensee and specifically aligning this computer with the software being licensed, the licensor is able to prevent unauthorized duplication of the licensed software. The licensor may allow the licensee to utilize the software on more than one computer, but in
30 this case, the licensor is able to specifically determine the number of computers on which the software will be allowed to operate. For marketing purposes, the licensor may also allow the software to operate in a demonstration mode on computers other than the one(s) specifically identified and aligned with the licensed software.

In contrast to prior art, the approach of this invention results in a very low cost per licensee for controlling the distribution of licensed software. The license registration process is fully automated, eliminates the need for additional encryption software or telephone calls to and from the user to obtain validation numbers or the like.

5 The registration process itself is almost completely transparent to the user, and the system provided is easy to integrate into existing applications. At the licensor's option, the registration process can be completely anonymous, protecting the licensee's right of privacy by not requiring personal data as a condition of being licensed to use the software.

10 In the preferred embodiment the use of the licensed software is restricted to one computer; however, the licensor may choose to provide the licensee with additional license(s) for back-up purposes, and/or to also utilize the software on a specific number of additional computers -- such as a portable computer or on multiple computers in homes, offices and other settings. Once the software has been loaded on the maximum
15 number of computers allowed by the licensor, and until the licensee obtains additional license(s), the software may be authorized to be utilized on additional computers in a demonstration mode. The demonstration mode generally will be a less than fully functional version of the original version, because it will contain only a subset of the features of the fully functional version, or will only work for a short period of time in a
20 fully functional mode.

In a preferred embodiment a method of controlling reproduction of software by an end user of the software includes providing to an entity that licenses its software to users, license generation software which, when operated, generates validation numbers, there being a unique validation number for each copy of the software to be
25 separately licensed. The validation number is included with the software when supplied from the licensor, and this number is incorporated with additional product information and provided to a license registration database.

When the user installs the software on the designated system(s), he registers the software by entering the validation number, plus a password that he creates.
30 At this time the system registration software, for example, as provided by AnchorSoft, also obtains the system identification number. This information is sent to the online Anchorsoft registration database, and, after successful verification, a license key is stored on the user's computer. This computer can now fully operate the licensed software.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram illustrating the process of registering a vendor's product with registration database;

Figure 2 is a diagram illustrating the licensing process employed in a preferred embodiment of this invention; and

Figure 3 is a diagram illustrating the online registration process.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

Figure 1 is a diagram illustrating the relationship between a vendor who provides software under license, and a service provider who implements a preferred embodiment of the system of this invention. The vendor is labeled as such, while the service provider is designated "AnchorSoft," a tradename of the assignee. The service provider creates a unique vendor identification number or designation (VID), a unique product identification number (PID), and a unique vendor encryption key (VEK). The service provider also maintains a library with product verification encryption keys (PVEK) and registration encryption keys (REK). In addition, the service provider has license generation software. The license generation software is software configured to accept the data referred to above, and in response generate a unique validation number for use with system of this invention.

As shown in Figure 1, the system registers a vendor's product by assigning a unique vendor identification number, a unique product identification number and a unique vendor encryption key. If the vendor is using the system to control licenses for more than a single product, the VID and VEK remain constant for that particular vendor; however, the PID will change to account for each new product.

The license generation software including the VID and VEK are provided to the vendor. In addition, the vendor also receives a product CD which contains a library including the PVEK, the REK, and the PID. To use the license generation software, the vendor enters the VID and the VEK. By doing so, the vendor is now ready to produce validation numbers and vendors' license numbers for use as described below.

As shown in Figure 2, the vendor generates software licenses in the following manner: The vendor uses the license generator software to generate licenses. Each license has two numbers, which are generated as a pair. The validation number

consists of a unique serial number (for this product) and a random number. The vendor's license number consists of the validation number plus the PID, VID, maximum number of license keys, and options. Options can be used, at the vendor's option, to enable certain features in the software product, set an upgrade 'timestamp', or other uses. The vendor's license number is encrypted using the vendor encryption key and is sent to AnchorSoft, where, after validation, it is inserted into the license database.

Next consider the end user. At the time the end user acquires the software from the retailer or other source, the end user receives the validation number accompanying that software. To register the software and "unlock" it for use on his computer(s), the user submits the validation number, together with a password chosen by the user to the software library through the registration option interface.

The software library combines this data with the system identification number (SID) to generate a "registration key." The user then contacts the license registration database at AnchorSoft by employing a web browser or other well-known modem software. The registration key is encrypted using the registration encryption key, and is then submitted to the license registration database. After successful verification of the registration key, the license database generates a license key, which consists of the PID, the SID and the options, and encrypts it using the product verification encryption key. The registration library receives the license key and stores it on the user's computer. If the verification library cannot verify the stored license key, then the software will, at the licensor's option, not operate, or only operate in demonstration mode.

As indicated by the figure, some of the information will be totally under the control of the end user, for example, the password. In contrast, other information, the system identification, will not be controlled at all by the end user, instead being provided from hardware in the user's computer. Examples of such hardware specific information include a unique number, such as the boot sector ID identifying the hard disk drive within the user's system, the network interface card ID, or a unique number identifying the microprocessor used in the system. Of course, if needed, another hardware dependent number identifying the user's computer can also be used provided it does not change frequently.

Although in the discussion above, the various numbers have been described as simple numbers, it will be appreciated that it is advantageous to employ encryption in establishing such numbers. In the preferred embodiment the Data

Encryption Standard (DES) is used. For security and verification purposes, the vendor license number, registration key and license key are all encrypted utilizing DES.

This invention employs a variety of numbers. These numbers and the components contained within each are as follows:

5

Validation number = serial number & random number.

10

Vendor's license number = validation number & vendor ID & product ID & number of registrations & options. Encrypted with the vendor encryption key.

Registration key = serial number & random number & product ID & SID & user password. Encrypted with the registration encryption key.

15

License key = product ID & SID & options. Encrypted with the product verification encryption key.

Each vendor has a unique vendor ID.

20

Each product has a unique product ID.

Each product has a registration encryption key and a product verification encryption key.

25

Different products may have identical serial numbers.

30

Figure 3 illustrates the manner in which the online registration process is performed. Steps performed by the user are shown with a small arrow beside them, while steps without an arrow are performed by the software in the license registration database. The user enters his validation number contained on his product and his self-generated password. The software library contained in the product verifies the validation number and obtains unique computer identification (typically the Ethernet number, processor serial number or boot drive ID). The software library creates a registration number and transmits this number to the AnchorSoft license registration database. The license registration database validates the registration number, stores the user password and creates a license key. The license key is transmitted back to the software library where it is stored in the user's system registry. The library will then display a successful registration message.

35

40

The system described above provides numerous advantages over prior art approaches. It eliminates loss of business caused by unauthorized duplication and distribution of licensed software by the user but still provides user with a fast and user friendly method of registration. The licensor is able to distribute his product in the partially disabled or time-limited demonstration version to potential buyers by placing the

demonstration version on CD-ROM or other media, or by allowing the product to be downloaded from an online venue. The licensor can encourage licensed users to distribute the demonstration copy to others and thus enjoy the benefit of any subsequent pass-along sales. The licensor can use the information from the license registration
5 database, to which AnchorSoft may provide access to the licensor, for sales tracking and forecasting.

The proceeding has been a description of the preferred embodiment of the invention. It will be appreciated that deviations and modifications can be made without departing from the scope of the invention, which is defined by appended claims.

10